SYSTEM SAFETY PROGRAM PLAN

FOR THE

EARTH OBSERVING SYSTEM (EOS)

CHEMISTRY PROJECT

JUNE 1999

GODDARD SPACE FLIGHT CENTER
GREENBELT, MARYLAND

FOREWORD

The Safety Plan describes the safety tasks to be conducted and assigns responsibility for each. The plan identifies the safety organizational structure and the standard procedures and instructions to be applied.

This document is not a direct instruction to NASA Contractors or others outside the EOS CHEMISTRY Project, but provides management guidance to the Project Personnel.

This is a Project Office Controlled Document. Changes require prior approval of the Project Manager. Proposed changes shall be submitted to the EOS CHEMISTRY Project Configuration Management Officer (Code 424).

Prepared by: **Signature of** 6/8/99
Richard W. Stickle, CSP, PE — Date
EOS System Safety Engineer
Hernandez Engineering, Inc.

Reviewed by: **Signature of** 6/8/99
Richard B. Bolt, PE — Date
EOS Project Safety Manager

Reviewed by: **Signature of** 6/8/99
Ronald Perison — Date
EOS CHEMISTRY Project
Systems Assurance Manager

Approved by: **Signature of** 6/24/99
Philip Sabelhaus — Date
EOS CHEMISTRY Project Manager

Goddard Space Flight Center
Greenbelt, Maryland

CHANGE RECORD PAGE

DOCUMENT TITLE: System Safety Program Plan for the EOS CHEMISTRY Project

DOCUMENT DATE: June 1999

ISSUE	DATE	PAGES AFFECTED	DESCRIPTION
Original	6/99	ALL PAGES	Approved by CCR #424-11-12-005

DOCUMENT TITLE: System Safety Program Plan for the EOS CHEMISTRY Project

RELEASE DATE: June 1999

LIST OF AFFECTED PAGES

Page No.	Revision	Page No.	Revision	Page No.	Revision
Cover	Original				
Title	Original				
i	Original				
ii	Original				
iii	Original				
iv	Original				
v	Original				
vi	Original				
1-1	Original				
1-2	Original				
2-1	Original				
3-1	Original				
3-2	Original				
3-3	Original				
3-4	Original				
4-1	Original				
4-2	Original				
4-3	Original				
4-4	Original				
4-5	Original				
4-6	Original				
5-1	Original				
5-2	Original				
5-3	Original				
5-4	Original				
5-5	Original				
5-6	Original				
5-7	Original				
5-8	Original				
5-9	Original				
6-1	Original				
6-2	Original				

TABLE OF CONTENTS

FIGURES

SECTION 1

INTRODUCTION

1.1 Purpose

The purpose of this System Safety Plan is to assure that all Project Safety responsibilities in program management, system acquisition, and mission execution are successfully discharged and that personnel, equipment, and facilities are protected against hazardous conditions. This document provides guidelines for preventing, managing, and controlling safety hazards throughout the mission.

1.2 Scope

This System Safety Plan encompasses the activities required for satisfying and demonstrating compliance with all safety requirements that apply to the design, fabrication, assembly, handling, transportation, verification, integration, ground operations, and launch phases of the mission elements. This plan outlines the approach and the responsibilities of organizational elements within the project for implementing the project's safety program.

1.3 List of Acronyms

CDR	Critical Design Review
CDCR	Conceptual Design and Cost Review
CDRL	Contract Data Requirements List
CFR	Code of Federal Regulations
CSP	Certified Safety Professional
DID	Data Item Description
DOT	Department of Transportation
ELV	Expendable Launch Vehicle
EOS	Earth Observing System
EPA	Environmental Protection Agency
FMEA	Failure Mode and Effects Analysis
GFE	Government-Furnished Equipment
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
HR	Hazard Report
MAR	Mission Assurance Requirements

NASA	National Aeronautics and Space Administration
NCR	Noncompliance Report
OSHA	Occupational Safety and Health Act
PAR	Product Assurance Requirements
PDR	Preliminary Design Review
PE	Professional Engineer
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PM	Project Manager
PSE	Project Safety Engineer
PSM	Project Safety Manager
SAM	Systems Assurance Manager
SAR	Safety Assessment Report
SCDP	Safety Compliance Data Package
SHA	System Hazard Analysis
SSA	Software Safety Analysis
SSIP	System Safety Implementation Plan
SSRP	System Safety Review Panel
SSWG	System Safety Working Group
WSMC	Western Space and Missile Center

SECTION 2

APPLICABLE DOCUMENTS

The following documents of the latest issue form a part of this plan to the extent specified herein and are applicable to this mission:

EWR 127-1 (T)	Range Safety Requirements (Tailored).
MIL-STD-882	System Safety Program Requirements.
MIL-STD-1522	Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems.
NPD 8700.1	NASA Policy for Safety and Mission Success
NHB 1700.1(V1-B)	NASA Safety Policy and Requirements Document.
MSFC-SPEC-522	Design Criteria for Controlling Stress Corrosion Cracking.
NPD 8710.2	NASA Safety and Health Program
GMI 1700.3	Systems Safety for Orbital Flight Projects.
GPG 7120.2	Project Management.
GSFC 424-11-13-01	Mission Assurance Requirements for the High Resolution Dynamics Limb Sounder (HIRDLS) for the EOS Chemistry Mission
GSFC 424-11-13-02	Mission Assurance Requirements for the Tropospheric Emission Spectrometer (TES) and the Microwave Limb Sounder (MLS) for the EOS Chemistry Mission
GSFC 424-11-13-03	Mission Assurance Requirements for the Ozone Monitoring Instrument (OMI) for the EOS Chemistry Mission
GSFC 424-11-13-05	Mission Assurance Requirements for the Ozone Monitoring Instrument (OMI) Interface Adapter Module (IAM) for the EOS Chemistry Mission
GSFC 420-05-04	Performance Assurance Requirements for EOS Common Spacecraft.
29 CFR 1910	Occupational Safety and Health Administration, Dept. of Labor, Part 1910.

29 CFR 1960 Basic Elements for Federal Employee OSHA Programs and Related Matters.

Others as specified by individual contract and those documents listed as required in the System Safety Implementation Plan

SECTION 3

GLOSSARY OF TERMS/DEFINITIONS

ACCIDENT/INCIDENT - An unplanned event that results in personnel fatality or injury: damage to, or loss of, carrier, experiments, environment, public property, or private property; or could result in an unsafe situation or operational mode. An accident refers to a major event, whereas an incident is a minor event or episode that could lead to an accident.

CERTIFICATE OF SAFETY COMPLIANCE - A formal documented statement of the safety assessment effort. It includes a statement that all safety requirements have been met or, if not, which noncompliance reports are applicable.

CORRECTIVE ACTION - Action taken to preclude occurrence of an identified hazard or to prevent recurrence of a problem.

CREDIBLE - A condition that can occur and is reasonably likely to occur.

EMERGENCY - Any condition that can result in injury or threat to life and requires immediate corrective action, including a predetermined response.

FAIL SAFE - A design feature that ensures that the system remains safe or in the event of a failure will cause the system to revert to a state which will not cause a mishap.

FAILURE - The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.

GSE (GROUND SUPPORT EQUIPMENT) - Includes electrical ground support equipment (EGSE) and mechanical ground support equipment (MGSE) that support the operation, testing, interface verification, verification, assembly, integration, transportation, launch and refurbishment of the flight equipment and its associated Airborne Support Equipment (ASE).

HAZARD - The presence of a risk situation. A condition that is prerequisite to a mishap.

HAZARD ANALYSIS - The technique used to systematically identify, evaluate, and resolve hazards.

HAZARD PROBABILITY - The aggregate probability of occurrence of the individual events that create a specific hazard.

HAZARD SEVERITY - An assessment of the consequences of the worst credible mishap that could be caused by a specific hazard.

HAZARDOUS MATERIAL - Anything that due to its chemical, physical, or biological nature causes safety, public health, or environmental concerns that result in an elevated level of effort to manage.

INDEPENDENT INHIBIT - Two or more inhibits are independent if a single event or environment cannot eliminate more than one inhibit, and all inhibits cannot be removed by the same type of event or environment.

INHIBIT - A design feature that prevents operation of a function.

MISHAP - An unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment.

MONITOR - Ascertain the safety status of payload functions, devices, inhibits, and parameters.

NONCOMPLIANCE REPORT - The documentation of a specific case of noncompliance with the requirements of the appropriate safety documentation.

PAYLOAD - An integrated assemblage of subsystems designed to perform a specified mission in space. It, therefore, includes items such as free flying automated spacecraft, individual experiments and instruments.

PAYLOAD ELEMENTS - Experiments, instruments or other individual payload items that are subsets of an integrated, multi-payload cargo complement.

PROJECT SAFETY REQUIREMENTS - Includes the contractually imposed design and operational requirements listed in compliance documents or system specifications, defines system constraints and capabilities, establishes acceptable or unacceptable risk conditions, and identifies specific design and operational criteria and approaches.

RESIDUAL HAZARD - Hazard for which safety or warning devices and/or special procedures have not been developed or provided for counteracting the hazard.

RISK - An expression of the possibility/impact of a mishap in terms of hazard severity and hazard probability.

RISK ASSESSMENT - A comprehensive evaluation of the risk and its associated impact.

SAFETY - Freedom from chance of personnel injury or fatality, and damage to or loss of equipment or property.

SAFETY CRITICAL - A term applied to a condition, event, operation, process or item of whose proper recognition, control, performance or tolerance is essential to safe system operation or use; e.g., safety critical function, safety critical path, safety critical component.

SAFING - (1) Action to retreat from an armed condition.
(2) Actions that eliminate or control hazards.

SYSTEM - A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement.

SYSTEM LOSS - Damage to an extent that renders repair impractical. Requires salvage or system replacement.

SYSTEM SAFETY - The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

SYSTEM SAFETY ENGINEER - An engineer who is qualified by training and/or experience to perform system safety engineering tasks.

SYSTEM SAFETY ENGINEERING - An engineering discipline requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated risk.

SYSTEM SAFETY GROUP/WORKING GROUP - A formally chartered group of persons, representing organizations initiated during the system acquisition program, organized to assist the program manager in achieving the system safety objectives. Regulations of the military components define requirements, responsibilities, and memberships.

SYSTEM SAFETY MANAGEMENT - A management discipline that defines system safety program requirements and ensures the planning, implementation and accomplishment of system safety tasks and activities consistent with the overall program requirements.

SYSTEM SAFETY MANAGER - A person responsible to program management for setting up and managing the system safety program.

SYSTEM SAFETY PLAN - The combined tasks and activities of system safety management and system safety engineering implemented by acquisition project managers.

SYSTEM SAFETY PROGRAM PLAN - A description of the planned tasks and activities to be used by the Project to implement the required system safety program. This description includes organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

WAIVER - Granted use or acceptance of an article that does not meet the specified requirements.

SECTION 4

SAFETY PROGRAM ORGANIZATION

4.1 Project Organization

The Goddard Space Flight Center (GSFC) is the responsible payload organization for the EOS Project and as such, has the overall safety responsibility for the EOS CHEMISTRY Project.

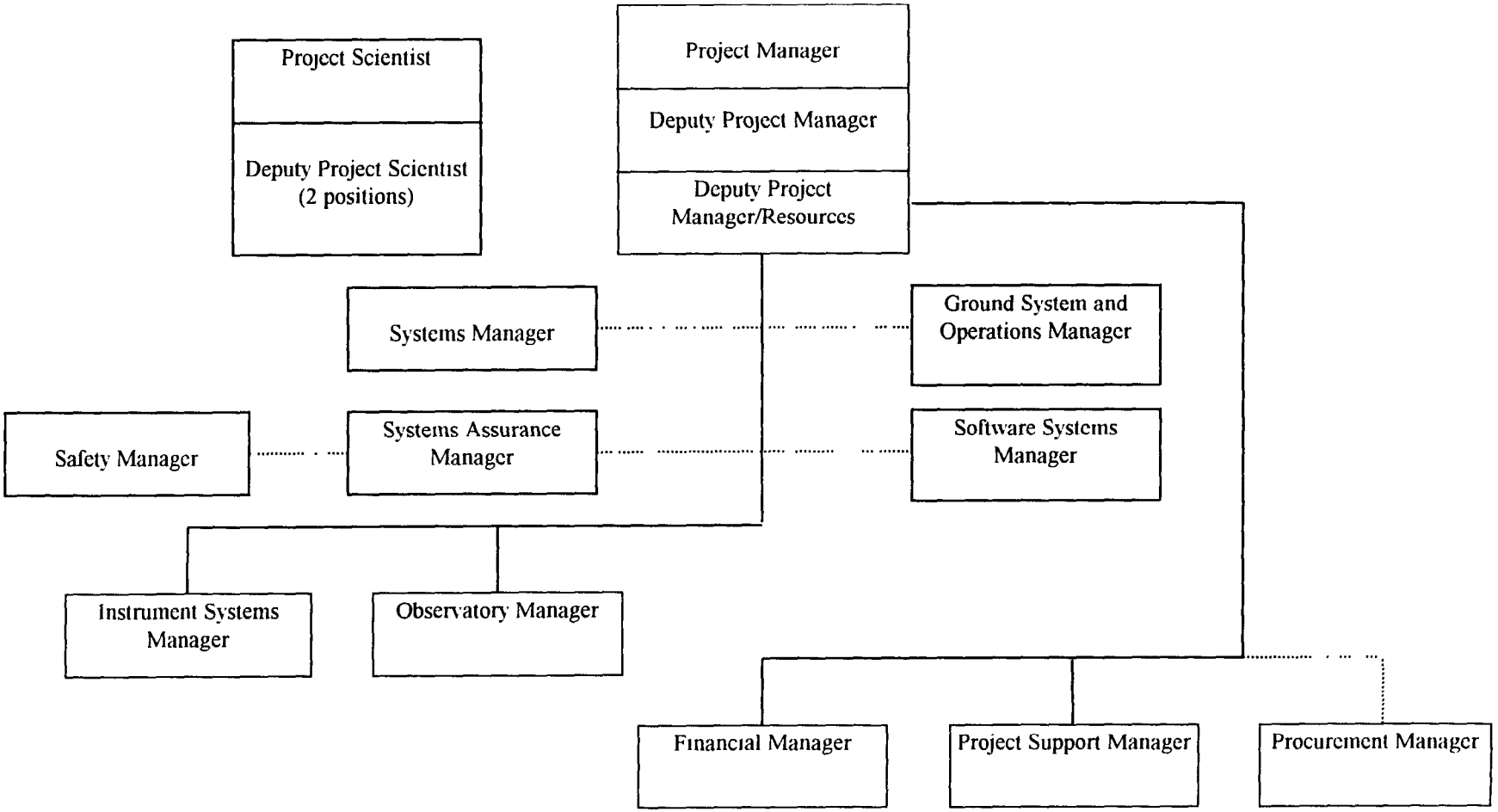
4.2 System Safety Organization

The primary responsibility of all EOS CHEMISTRY Project activities rests with the EOS CHEMISTRY Project Manager. Among these responsibilities are those to implement all EOS CHEMISTRY System Safety policies and to assure that identified risks are either eliminated or controlled on the EOS CHEMISTRY Project.

The technical aspects of the EOS CHEMISTRY System Safety program are directly supervised by the Project Safety Manager (PSM). In general, the PSM provides technical safety support to all design, test, and operations elements; prepares contractual safety documents; reviews and recommends approval of test and operations procedures; and participates in the presentation of the safety review process.

The specific System Safety activities are described in Section 5 of this document. Figure 4.1 shows the relationship of the System Safety function to other elements of the EOS organization. The PSM and Project Safety Engineer (PSE) assigned to the EOS CHEMISTRY Project possess the necessary qualifications and previous System Safety experience to perform the functions described herein.

CHEMISTRY PROJECT ORGANIZATION CHART
Figure 4.1



4.3 System Safety Interfaces/Responsibilities

4.3.1 Engineering Disciplines

The PSM interfaces directly with each engineering discipline that influences the safety of the EOS Chemistry spacecraft during its life cycle. The primary interface is with the system personnel and subsystem design elements but System Safety must also be coordinated with the software, procurement, reliability, system test, quality assurance, configuration management, mission operations, system requirements, and the system environment disciplines. A major element of these interfaces will be the tasking of the engineering disciplines by System Safety with engineering support activities. In addition to the criteria, analysis, and trade study activities discussed in subsequent paragraphs, System Safety engineering personnel and the EOS engineering disciplines will provide technical support to each other on a continuing basis. Technical support consists of consultation on safety-related problems, research of new product development, research/interpretation of safety requirements, specifications and standards. This activity does not duplicate hazard analysis efforts, but provides a timely and cost-effective method of assuring inherent safety in designs and operational planning.

4.3.2 Project Management Review

The PSM will participate in selected system-level status meetings, which will include Preliminary Design Review (PDR), Critical Design Review (CDR), Pre-Environmental Review (PER), and Pre-Ship Review (PSR). The System Safety presence at these status meetings allows for timely response to project decisions affecting safety and provides an effective forum for the presentation of System Safety program status, the identification of open safety items and concerns, and the assignment of action items to appropriate disciplines.

The safety review dates shall roughly coincide with those for the major program reviews (PDR, CDR, and PSR). The Safety Compliance Data Package(s) developed for the Air Force review panel will be presented in its entirety or in part as appropriate as a part of the safety presentations for EOS Chemistry in accordance with the Data Requirements List on the contract or working agreement. The status of all identified hazards will be assessed, and assigned hazard categories and recommended hazard control action will be provided as part of these presentations.

System Safety participation in all reviews also provides the safety program with management visibility to assure that:

(1) It complies with contractually imposed System Safety requirements.

(2) Safety program schedule and CDRL delivery dates are compatible.

(3) The necessary technical data is provided to permit preparation of the safety data package.

(4) System Safety concerns, hazard risks, and deviations are identified and receive appropriate attention.

(5) All safety issues arising during design reviews are documented and incorporated into a formal tracking system.

Participation in pre-environmental and pre-ship reviews provide final verification of the implementation of safety requirements, including mandatory task sequencing and availability of specified safety equipment.

4.3.3 System Safety Review Panel

The PSM organizes and chairs the System Safety Review Panel (SSRP). Membership to this committee includes the Project Manager or his designated representative, the Systems Assurance Manager (SAM), a systems engineer, subsystems engineers, and other disciplines as needed.

The purpose of the Committee is to technically evaluate the identified hazards in the EOS Chemistry system, Chemistry support equipment, and the associated operations, and to assure an acceptable level of safety. Each Committee member is responsible for assisting in the task of identifying and documenting individual hazards.

Meetings of the SSRP will commence as necessary prior to system PDR, when hazardous aspects of the developing system and subsystem designs can be identified. The meetings will continue until the hazard analyses are completed and comprehensive hazard list is fully compiled and approved. Meetings held after the issuance of the hazard list are on an as needed basis, e.g., as the System Test and Launch Operations phases of the program

encounter or reveal new hazards that require changes to operations.

The Committee reviews the safety documentation and presentations. Typical areas that will be addressed by the Committee in various reviews include:

a) Radiation safety (ionizing and non-ionizing).

b) Contractor safety activities, safety plans, and other safety documentation.

c) Interface safety relationships within the spacecraft/instruments system.

d) Personnel training and certification.

e) Precautions to prevent overtesting and operational errors during environmental testing.

f) Precautions to prevent electrostatic discharge damage.

g) Safety interface relationships with GSFC, integrating contractor, and the launch site.

h) Completeness of coverage of all potential hazards or hazard contributors and their resolutions.

i) Meeting of structural and fracture control requirements.

j) Materials compatibility.

k) Hazardous operations review.

l) Safety audits (required by Paragraph 5.3.4).

SECTION 5

SYSTEM SAFETY ELEMENTS

5.1 Hazard Risk Assessment

5.1.1 System Safety Criteria

5.1.1.1 Hazard Levels

A hazard level is assigned to each function in accordance with the definitions contained in table 5.1 below.

Hazard Severity Categories

Description	Category	Definition
CATASTROPHIC	I	Death, system loss, or severe environmental damage.
CRITICAL	II	Severe injury, severe occupational illness, major system or environmental damage.
MARGINAL	III	Minor injury, minor occupational illness, or minor system or environmental damage.
NEGLIGIBLE	IV	Less than minor injury, occupational illness, or less than minor system or environmental damage.

Table 5.1

5.1.1.2 Hazard Reduction

Management acceptance of credible risk is based upon the magnitude of the risk compared with the impact of compensating for it. The following hazard control steps, listed in preferential order, will be used by GSFC to eliminate or control hazards on the EOS CHEMISTRY Project:

1) Design for Minimum Risk - Hazards will be eliminated by design where possible. The major goal throughout the design phase will be to ensure inherent safety through the selection of appropriate design features as fail operational/fail safe combinations and appropriate safety factors. Damage control,

containment, and isolation of potential hazards will be included in design considerations.

2) Use of Safety Devices - Hazards that cannot be eliminated through design selection will be reduced to an acceptable level through the use of appropriate safety devices as part of the system, subsystem, or equipment.

3) Employ Warning Devices - Where it is not possible to preclude the existence or occurrence of a known hazard, devices will be employed for the timely detection of the condition and the generation of an adequate warning signal. Warning signals and their application will be designed to minimize the probability of wrong signals or of improper personnel reaction to the signal.

4) Use of Special Procedures - When it is not possible to reduce the magnitude of existing or potential hazards through design, or the use of safety and warning devices, special procedures will be developed to counter hazardous conditions for enhancement of personnel.

5.1.1.3 System Safety Design Criteria

System Safety design criteria will be developed and documented as an integral part of the EOS CHEMISTRY Program. These criteria will be used to guide the EOS design and will be included in all system and subsystem level requirements.

5.1.2 Trade Study Support

System Safety will participate in trade studies. Safety studies and analyses will be performed as appropriate to assess the relative accident potential of each trade alternative, or define minimum requirements for safety critical systems. System Safety will ensure that safety impact items and accident risk assessments are adequately highlighted and given appropriate weight as decision drivers. Program documentation will be reviewed to ensure that recommendations for management-level decisions include the optimum safety provisions consistent with program considerations and Western Space and Missile Center (WSMC) requirements.

5.1.3 Hazard Identification

A close and active participation in the design process is mandatory to properly implement an effective safety program. The design phase activities include:

1) Identification and elimination or control of hazards,

2) Development of effective safety criteria,

3) Implementation of these criteria and the verification of such implementation through the design review and approval process.

5.1.4 Hazard Control

Hazards will be identified by evaluation of the systems, subsystems, procedures, and operations against the safety criteria identified for the EOS CHEMISTRY Project. Identified hazards will be controlled and mitigated by the cognizant design organizations in concert with the PSM. Documentation of hazard controls on Hazard Reports (HR's) and verification of design and implementation of these controls will ensure the safety of the system. Hazard analysis shall be performed following the guidelines of MIL-STD-882. Safety hazards that are not totally controllable by the design action because of impact on cost, performance or schedule will be dealt with at the highest feasible order of precedence. Corrective action to be taken will be in the following order of precedence:

- Safety devices
- Protective systems
- Warning devices
- Special procedures

5.1.5 Hazard Analysis

5.1.5.1 General

The system safety analyses effort will be performed in an iterative and systematic manner to examine the system, subsystem, facilities, components, software, personnel, and their interrelationship including logistics, training, maintenance, tests, modification and operational environments. The analyses will identify hazards, evaluate, and assist the development of methods to eliminate and/or control the accident risk to an acceptable level.

5.1.5.2 Preliminary Hazard Analysis

A Preliminary Hazard Analysis (PHA) will be conducted early in the program to provide a comprehensive, qualitative safety assessment of the EOS CHEMISTRY system equipment and testing, in the intended operating environments. The hazard analysis will identify all potential hazards associated with the design, transportation, integration, testing, training, and operational modes.

5.1.5.3 System Hazard Analysis

System Safety will perform System Hazard Analyses (SHA) for the EOS Spacecraft that extends throughout all phases of the EOS Program. The SHA is a system and subsystem level qualitative analysis that identifies potential hazards and assures their resolution.

System Safety will assure that as a minimum each potential category I and II hazard is documented on a hazard report form. Each hazard report will:

a) Describe the potential hazard.

b) Show the hazard causes.

c) Identify the proposed hazard controls.

d) Relate the results of hazard control verification.

d) Provide tracability.

In all cases, the information provided will be concise with sufficient back-up data to ensure that each report can be a ▒ stand-alone▒ document. Where appropriate, the pertinent test reports, analyses, schematics, or materials data will be either summarized or attached to the report. The following paragraphs discuss each element of the hazard report in detail.

The hazard titles and descriptions are taken directly from the hazard list. A hazard can be described as a ▒ top▒ or ▒ end▒ event that could cause injury or damage to the system or the surrounding area.

As potential hazards are defined for the project during its preliminary design phase, the causes for each hazard will be identified. Causes are types or classes of events that can lead to the occurrence of the identified hazard. When necessary, or desired, individual causes may be sub-divided.
Hazard controls and the tracking procedure for each hazard will be proposed by PDR, and finalized by CDR. Controls are the specific means by which a design or procedure will prevent the cause of a hazard from occurring. Each identified cause will have a minimum of one control. The hazard report will provide sufficient means to verify that the hazard control is in place. In all cases, the goal of System Safety is to reduce the hazard to an acceptable risk level by employing proper controls.

Each hazard report will specify how and when its controls are to be verified prior to ground or flight operations. Although most verifications cannot be completed until after CDR, the eventual verification of hazard controls will be a consideration from the inception of the design phase. Verification of each identified hazard control in a hazard report is accomplished by System Safety review of test reports, engineering drawings, engineering analyses, procedures, training/certification plans, task flow charts, and /or surveillance of test and demonstrations. A hazard report will not be closed until verification of all the controls is complete.

All hazard reports will have tracability by providing specific source references for each control and verification approach.

Throughout the evolution of the hazard report, the identified hazard will be jointly resolved between the responsible functional element and the System Safety organization. Final closure of the report will occur when both the GSFC EOS Project Manager and the WSMC Safety Panel Chairperson approve the report, signifying concurrence with the hazard control and verification methods. Any residual risks from the hazard reports must have been accepted by WSMC. The rationale for acceptance of a residual hazard will always be documented on the hazard report and filed in the EOS Chemistry Library.

5.1.5.4 Software Safety Analysis

The object of the Software Safety Analysis (SSA) is to identify potential hazards to the EOS Chemistry Spacecraft, and related launch vehicle facilities and personnel. These June be external to the software system, such as erroneous or improperly timed commands, and internal to the software system, such as computer commands causing illegal entry into critical routines. The results of the SSA will be used to:

a) Influence the design of the software whenever practical to assure control of possible system hazards.

b) Identify in the appropriate hazard reports those potential hazards introduced or impacted by the software systems.

System Safety will, with the aid of the Software Management personnel, conduct a SSA as a portion of the system hazard analysis. For the purposes of this section, the term software system will include the system specification, computer programs, the computers, and all of the peripheral equipment that enables the system to operate. The SSA will be performed on all software having direct interface with EOS safety critical hardware systems and will be performed during the software design and development. The following areas will be evaluated depending on the development phase:

1. Software Requirements - Analyze the software requirements to ensure all unsafe modes are avoided; e.g., hazardous commands must be verified prior to execution, appropriate error/exception handling.

2. Software Test - Assure test plans and procedures are developed to adequately test safety requirements and review test results.

3. Review user, operations, and maintenance manuals for inclusion of safety related information as appropriate.

5.1.5.5 Related Analyses

Analyses developed by other disciplines [e.g., Failure Mode and Effects Analysis (FMEA), Trade Studies, etc.] will be used by the System Safety Engineers to aid in the identification of failure points that present an accident risk. Hazards identified by these sources will be addressed in the hazard reports.

5.1.6 Noncompliance Reports

Compliance with all applicable NASA and Air Force safety criteria contained in Section 2.0 is mandatory unless exceptions are granted by NASA or the Air Force. Noncompliance with any design, documentation, software or procedure requirement will necessitate the preparation of a Noncompliance Report. Each Noncompliance Report will be limited to a specific subsystem or component in a specific application.

When they are required, noncompliance reports will be prepared as early in the timeline as possible. The report will be prepared by the responsible engineering section and routed to the EOS Project System Safety Engineer for review. Final approval of safety waivers and deviations remains the responsibility of the launch site safety organization.

5.1.7 Engineering Change Proposal (ECP)

System Safety will participate in all applicable configuration control activities to provide review and concurrence with all engineering design or procedure changes. Each proposed change to an approved design will be reviewed to determine if a system safety assessment is required as part of the EOS Chemistry Change Configuration Board process.

5.1.8 Post-Flight Evaluation

System Safety will participate in post-flight reviews and a safety evaluation will be made in cases where anomalous conditions are revealed. This safety evaluation will provide guidance in planning future missions and establishing necessary corrective action to reduce hazards.

5.2 Launch Complex Safety

This subsection of the EOS CHEMISTRY Project System Safety Plan addresses the means by which GSFC plans to implement the general safety policies of the launch complex.

5.2.1 Test and Operating Procedures

The closed-loop process of the System Hazard Analysis ensures incorporation of system safety requirements in the appropriate test and operations procedures. The SHA considers both the adequacy of testing to assure future safe operation, and the safe test performance, including provision of adequate protective and support equipment. The safety compliance data package submitted by System Safety will provide a summary listing of all applicable procedures and step numbers that control potential hazards identified in the SHA.

Each test, operating, or maintenance procedure or computer-controlled test sequence to be conducted for the EOS CHEMISTRY Program will be reviewed and approved by System Safety. The review will be based on the results of the hazard analyses. Signature approval of each hazardous procedure will be provided when the procedure meets all safety requirements and contains the appropriate caution and warning notations.

When a launch complex procedure has been designated as hazardous by the Project, the procedure must have launch site approval prior to use and always after the Project's safety approval. Any deviation at any time from an approved safety-critical procedure will require reassessment of the procedure and approval by System Safety, the Project, and the launch complex.

5.2.2 Hazardous Operations Surveillance

Test and operations activities at the launch site will be monitored by System Safety to ensure implementation of safety requirements and the use of appropriate personnel protective equipment. Continuous surveillance will be provided for hazardous operations. System Safety and/or Industrial Safety will have the authority to disprove all real-time procedure deviations and/or halt operations when an unacceptable hazardous situation will result or exists. This monitoring will be supplemented by routine inspections of test and facility hardware to ensure that unsafe conditions do not exist.

5.2.3 Training and Certification

The EOS CHEMISTRY Project will arrange and/or provide any required training or certification for project personnel who are to be involved in ground processing operations at the launch site.

Certification encompasses personnel technical knowledge, formal (systems and skills) training courses, on-the-job training, verification of skills, and demonstration of individual capabilities. Medical examinations will be required for specific certifications.

5.2.4 Safety Audits

Internal Safety audits will be conducted by the Project System Safety Review Panel periodically. The committee will be composed as outlined in Paragraph 4.3.3. Other members June be appointed if specialists are required in conducting the safety assessment. This committee will meet for an initial safety assessment of the science payload and for a final safety certification. Other meetings are to be called as necessary to insure proper completion of the safety analysis tasks before submission of safety compliance review packages to the launch site. All findings will be reported to the EOS Chemistry Project Manager and the GSFC System Safety Branch.

5.2.5 Accident Investigation and Reporting

The investigation and reporting of accidents/incidents involving NASA hardware, software, or GSE will be performed in accordance with NHB 1700.1, NASA Safety Manual, Volume 1, and NASA Management Instruction, NPD 8621.1, Mishap Reporting and Investigating. The EOS CHEMISTRY Project will support a NASA accident investigation by providing records, data, and administrative/technical assistance requested by the investigating board.

An accident report containing all pertinent data will be prepared and included in the safety documentation file. All accidents will be assessed for ground and flight safety impact, and the summary of these assessments will be documented in the Safety Compliance Data Package.

5.3 Monitoring of Contractors

Subcontractors to the EOS CHEMISTRY Project will be required by contract to submit the necessary hazard analyses, materials lists, certifications, and other data as required to satisfy the requirements of EWR 127-1 (T), GSFC 420-05-04 and other pertinent safety documents.

5.4 Contractor System Safety Plans

Where a contractor to GSFC is involved with procurement and delivery of flight hardware, the contractor will prepare a system safety plan. The plan must be individually tailored to the specific hardware being produced. The system safety plan will be submitted to GSFC for review and approval as required by the appropriate EOS Project Mission Assurance Requirements (MAR) document.

SECTION 6

INDUSTRIAL SAFETY ELEMENTS

The GSFC Health, Safety, and Security Office is responsible for several tasks associated with any EOS fabrication and testing at GSFC. These tasks are identified in the following paragraphs and all will be performed in compliance with local, state, and federal safety regulations. The EOS PSM will be the primary point of contact with non-GSFC sites.

6.1 Review/Approval of Purchase Requisitions for Hazardous Materials

All hazardous materials purchased will be approved by the Health, Safety, and Security Office. Before approving a requisition, the Health and Safety Engineer will determine if the organization requesting the material has adequate storage, proper job training or certification to use the hazardous material, a need for additional licensing or approvals, a need for additional usage facilities, and adequate procedures for proper control.

6.2 Review/Approval of Hazardous Manufacturing Processes

All hazardous manufacturing process documentation will have safety input to the rough draft, approval on the final draft and revisions, and for certain selected processes, a final validation. The following aspects will be considered:

1) All hazardous materials will be reviewed as to their necessity. Control, storage, and particular skills necessary to safely handle these materials will be reviewed.

2) Protective clothing, equipment, and requirements will be added as necessary.

3) Environmental health aspects will be added as required.

4) A specific safety section will be written if required.

6.3 Review/Approval of Facility and Tool Drawings

All facility drawings and specific tool drawings that affect transportation, handling, or lifting/pressurization devices will be reviewed and approved by the Health, Safety, and Security Office. Compliance with existing procedures and regulations regarding fire prevention and evacuation, illumination, noise, and other industrial safety hazards will be verified during these reviews.

6.4 Review/Approval of Test Procedures and Test Monitoring

The GSFC Health, Safety, and Security Office representative has the prerogative to participate in procedure review and approval meetings, and in test and validation operations involving risk to personnel, system hardware, and/or facilities. The Safety Engineer will provide surveillance during the conduct of hazardous operations to assure compliance with procedures and regulations. Pretest safety inspections will be conducted by the Safety Engineer to assure that the operating environment is free from hazards.

6.5 Safety Training and Certification

Test and operational personnel will be required to complete training courses for critical or hazardous operations and prerequisites for personnel certification. All training courses will contain institutional safety inputs to emphasize critical or hazardous functions or operations.

Certification is granted based on personnel technical knowledge, accomplishment of formal (systems and skills) training courses and on-the-job training, verification of skills, and demonstration of individual capabilities. Medical examinations may also be required for certain skill certifications.

6.6 Fire Prevention

All ordnance, propellants, chemical and other hazardous material storage areas, as well as manufacturing, test, and office work areas, will be protected by either automatic fire detection and suppression equipment, or by 24-hour security surveillance, or both as appropriate.